KOMISIJI ZA STUDIJE II STEPENA ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena, Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 12.05.2015. godine imenovala nas je u Komisiju za pregled i ocenu master rada dipl. inž. Kovačević Lazara pod naslovom „SystemC modelovanje bloka za enkripciju i dekripciju po GCMP protokolu". Nakon pregleda materijala Komisija podnosi sledeći

IZVEŠTAJ

1. Biografski podaci o kandidatu

Lazar Kovačević je rođen 11.07.1990. godine u Čačku. Pohađao je osnovnu školu u Guči i Gimnaziju u Čačku, prirodno-matematički smer. Upisao se na osnovne akademske studije na Eletrotehničkom fakultetu u Beogradu 2009. godine. Diplomirao je 10. oktobra 2013. godine na modulu Elektronika, sa prosečnom ocenom 8,07 i ocenom 10 na diplomskom radu. Master studije na Elektrotehničkom fakultetu u Begradu upisao je 2013. godine na odseku za Elektroniku. Položio je sve ispite sa prosečnom ocenom 10.

2. Opis master rada

Master rad kandidata sadrži 68 strana sa dodacima. Rad sadrži šest poglavlja i spisak literature sa dvanaest referenci.

Prvo poglavlje predstavlja uvod u kome su opisani predmet rada, cilj i struktura.

U drugom poglavlju dat je opis bezbednosnog protokola GCMP (*Galois Counter Mode Protocol*) po standardu IEEE 802.11ad-2012. Ovim standardom se definiše novi fizički sloj tako da se bežična komunikacija može vršiti na centralnoj učestanosti od 60 GHz sa propusnim opsegom od 2160MHz i protokom do 7GBit/s. Opisani su algoritmi koje ovaj bezbednosni standard koristi (GCM i AES) i prikazan je odgovarajući matematički aparat. Na kraju je dat predlog implementacije bloka za enkripciju i dekripciju po GCMP protokolu.

U trećem poglavlju je prvo ukratko opisan SystemC, jezik za projektovanje i verifikaciju hardvera. Potom su objašnjene metodologije za projektovanje digitalnih sistema korišćenjem SystemC-a. Na kraju je predstavljena metodologija koja je korišćena u ovom radu za projektovanje bloka za enkripciju i dekripciju po GCMP protokolu.

Četvrto poglavlje sadrži opis arhitekture projektovanog GCMP bloka. Prvo je opisan blok u celini, a zatim je dat opis svih podblokova koji predstavljaju funkcionalne algoritamske celine. Opisane su odgovarajuće mašine stanja, a njihovi dijagrami stanja su dati u prilogu rada kao dodatak.

U petom poglavlju je dat opis verifikacionog okruženja u kome je projektovani blok testiran. Opisan je *testbench*, a zatim je dat opis same simulacije. Objašnjena je mogućnost ponovne upotrebe simulacije koju pruža SystemC i alat korišćen za simulaciju. Na kraju su prezentovani rezultati simulacije i prikazani vremenski dijagrami kojima je verifikovana funkcionalnost projektovanog GCMP bloka.

Na početku šestog poglavlja je definisan pojam sinteze visokog nivoa kojom se od SystemC modela može generisati RTL model hardvera. Zatim je objašnjena karakterističnost te sinteze za *CtoS* (*C to Silicon*), alat koji je korišćen u ovom radu. Na kraju su prikazani rezultati sinteze visokog nivoa za GCMP blok i analiziran je kvalitet dobijenog RTL modela.

Na kraju rada je dat zaključak.

3. Analiza rada sa ključnim rezultatima

Master rad dipl. inž. Lazara Kovačevića se bavi primenom metodologije projektovanja digitalnih elektronskih sistema koja omogućava modelovanje sistema na visokom nivou apstrakcije i pruža mogućnost istovremenog projektovanja hardverskih i softverskih elemenata sistema. U radu je korišćen SystemC kao jedan od trenutno najzastupljenijih jezika koji pruža takve mogućnosti. Modelovan je blok za enkripciju i dekripciju podataka po GCMP protokolu koji je definisan standardom 802.11ad-2012 za bežične uređaje. Najveći izazov u pomenutoj metodologiji predstavlja postupak sinteze visokog nivoa kojom od SystemC modela treba generisati RTL model hardvera. Tome je u radu posvećena posebna pažnja i prikazani su rezultati koji potvrđuju uspešnost tog koraka u projektovanju GCMP bloka korišćenjem *CtoS* alata za sintezu visokog nivoa.

Najvažniji doprinosi master rada su:

- prikaz savremene metodologije projektovanja digitalnih sistema korišćenjem SystemC jezika,
- analiza bezbednosnog GCMP protokola definisanog standardom 802.11ad-2012 čija se masovna primena u bežičnim uređajima široke potrošnje očekuje tek za nekoliko godina,
- uspešno modelovanje bloka za enkripciju i dekripciju podataka po GCMP protokolu postignuto primenom opisane metodologije,
- prikaz sinteze visokog nivoa korišćenjem *CtoS* alata i uspešno generisanje RTL modela GCMP bloka.

4. Zaključak i predlog

Kandidat Lazar Kovačević je u svom master radu uspešno modelovao GCMP blok za enkripciju i dekripciju podataka po 802.11ad-2012 standardu korišćenjem SystemC jezika.

Na osnovu gore navedenog Komisija predlaže Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da prihvati rad „SystemC modelovanje bloka za enkripciju i dekripciju po GCMP protokolu“ dipl. inž. Kovačević Lazara kao master rad i odobri javnu usmenu odbranu.

U Beogradu, 28.08.2015.

Članovi komisije:

dr Jelena Popović-Božović, doc.

dr Nenad Jovičić, doc.